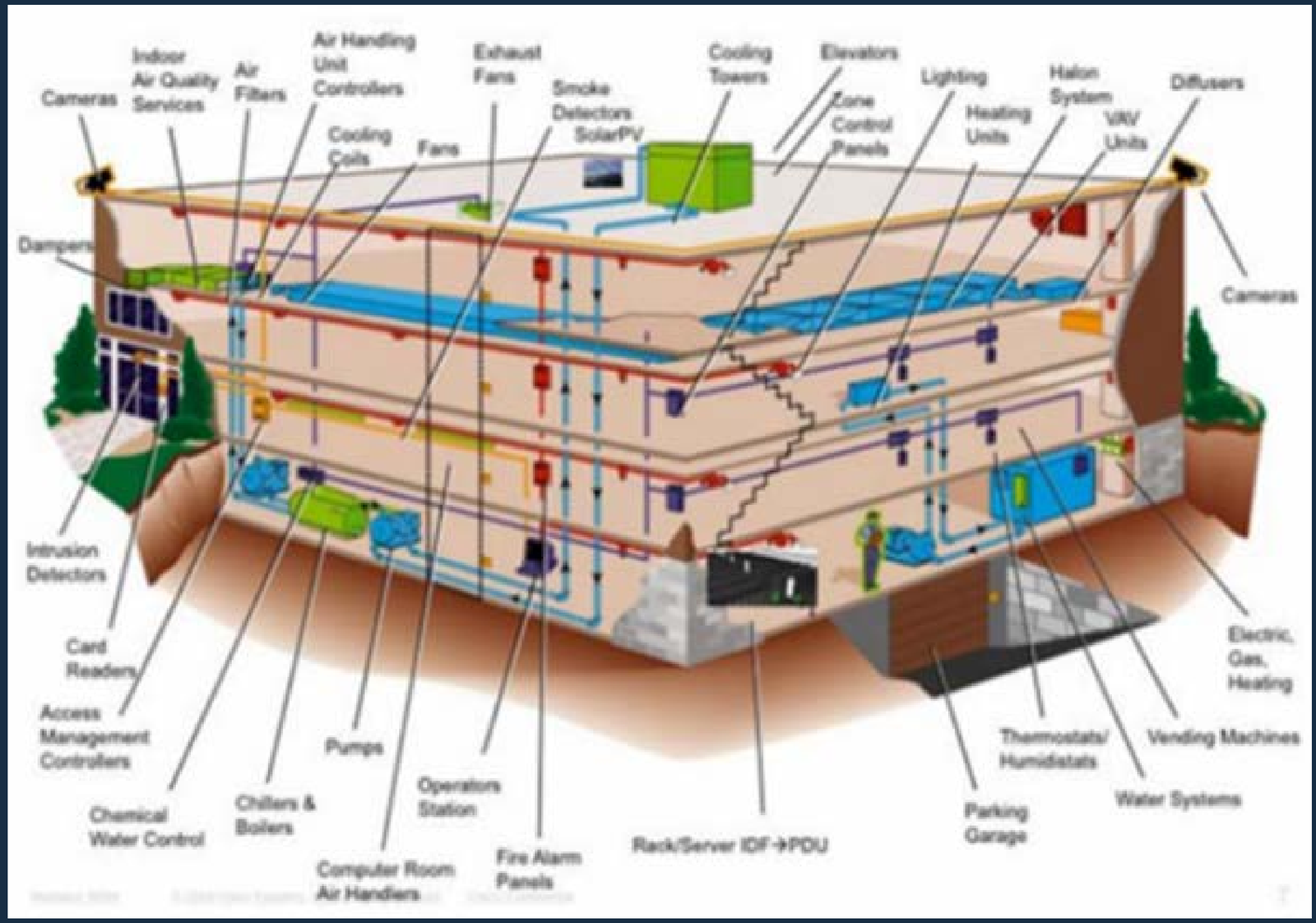
Control Systems Cybersecurity Who's Monitoring Your Infrastructure Networks?



Prepare for a World of Incessant, Relentless & Omnipresent Cyber Conflict in Every Aspect of Our Daily & Commercial Lives

"Bottom line: time to brush up on Iranian TTPs and pay close attention to your critical systems, particularly ICS," Krebs said. "Make sure you're also watching third party accesses!"

US Govt Says Iran's Cyberattacks Can Disrupt Critical Infrastructure. DHS warned in a terrorism threat alert via National Terrorism Advisory System (NTAS} that cyberattacks carried out by Iranian-backed actors against U.S. have potential to disrupt critical infrastructure. Iran and partners such as Hizballah, have demonstrated intent & capability to conduct operations in U.S., with previous such efforts having included, among other things, scouting & planning against infrastructure targets and cyber-enabled attacks against a range of U.S.-based targets.

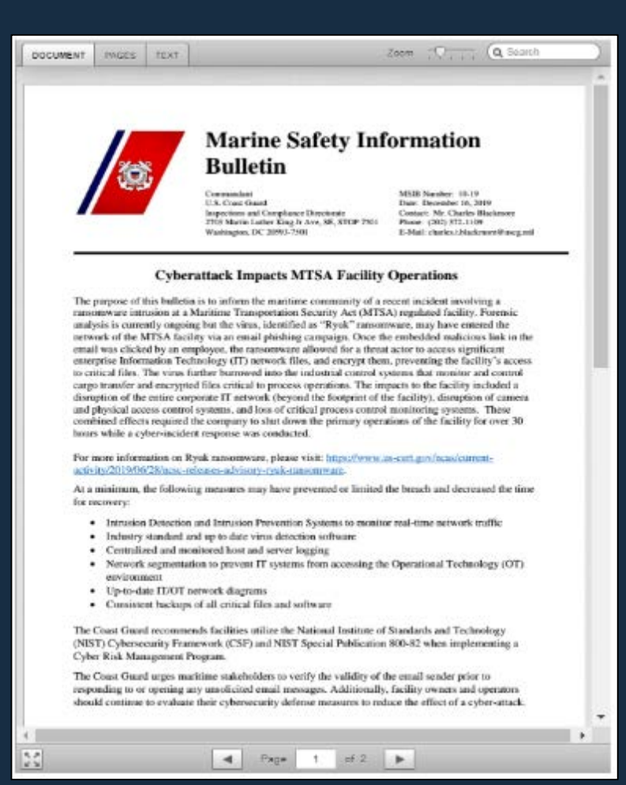
Chemical / Commercial Facilities / Communications / Critical Manufacturing / Dams / Defense Industrial Base / Emergency Services / Energy / Financial Services / Food & Agriculture / Government Facilities / Healthcare and Public Health / Information Technology / Nuclear Reactors, Materials & Waste / Transportation Systems / Water and Wastewater Systems

Ryuk Ransomware Strikes Again

Ryuk used to infiltrate computer networks at marine transportation facility through phishing an employee, causing an outage of roughly 30 hours, the U.S. Coast Guard said in a recent security advisory.

"The virus burrowed into the ICS that monitor and control cargo transfer and encrypted files critical to process operations"

DHS Cybersecurity and Infrastructure Security Agency flagged a National Cyber Security Centre advisory about Ryuk in June



DOCUMENT | IMAGES | TEXT — Zoom — Search

Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 10-19
Date: December 16, 2019
Contact: Mr. Charles Blackmore
Phone: (202) 372-1109
E-Mail: charles.l.blackmore@uscg.mil

Cyberattack Impacts MTSA Facility Operations

The purpose of this bulletin is to inform the maritime community of a recent incident involving a ransomware intrusion at a Maritime Transportation Security Act (MTSA) regulated facility. Forensic analysis is currently ongoing but the virus, identified as "Ryuk" ransomware, may have entered the network of the MTSA facility via an email phishing campaign. Once the embedded malicious link in the email was clicked by an employee, the ransomware allowed for a threat actor to access significant enterprise Information Technology (IT) network files, and encrypt them, preventing the facility's access to critical files. The virus further burrowed into the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations. The impacts to the facility included a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critical process control monitoring systems. These combined effects required the company to shut down the primary operations of the facility for over 30 hours while a cyber-incident response was conducted.

For more information on Ryuk ransomware, please visit: https://www.us-cert.gov/ncas/current-activity/2019/08/28/ncsc-releases-advisory-ryuk-ransomware.

At a minimum, the following measures may have prevented or limited the breach and decreased the time for recovery:

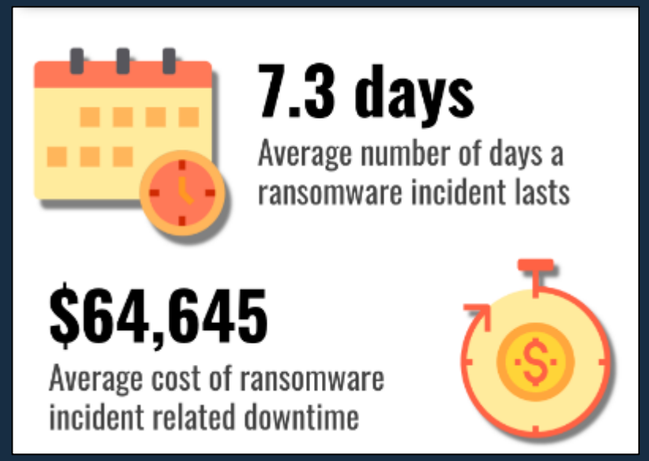
- Intrusion Detection and Intrusion Prevention Systems to monitor real-time network traffic
- Industry standard and up to date virus detection software
- Centralized and monitored host and server logging
- Network segmentation to prevent IT systems from accessing the Operational Technology (OT) environment
- Up-to-date IT/OT network diagrams
- Consistent backups of all critical files and software

The Coast Guard recommends facilities utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82 when implementing a Cyber Risk Management Program.

The Coast Guard urges maritime stakeholders to verify the validity of the email sender prior to responding to or opening any unsolicited email messages. Additionally, facility owners and operators should continue to evaluate their cybersecurity defense measures to reduce the effect of a cyber-attack.

Page 1 of 2

- **WIZARD SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018**
  - **Targeting large organizations for a high-ransom return**
  - **Russia-based group known for the operation of the TrickBot banking malware that focused primarily on wire fraud in the past**
- **Since Ryuk's appearance, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD**



Source: Coveware

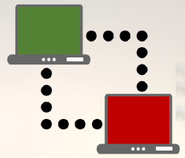
Over 100 US businesses have been targeted by Ryuk

THE CYBER LANDSCAPE

UNCLASSIFIED

NETWORK & INFO SHARING

End point mgmt:
- *Perimeter defense*
- *Comply to connect*
- *Continuous monitoring*



Identity, credential, and access mgmt

DevSecOps

NETWORK REMEDIATION

CYBER WORKFORCE

CROSS DOMAIN

Mission Partner Networks

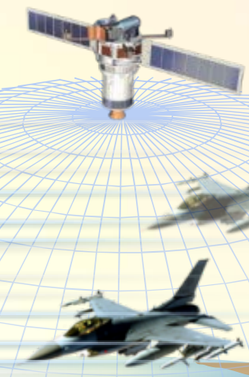
ENCRYPTION

Artificial Intelligence

The Cloud

ENABLERS

POSITIONING, NAVIGATION, AND TIMING



WEAPON SYSTEMS

COMMAND, CONTROL, AND COMMUNICATIONS

HUMAN FACTORS

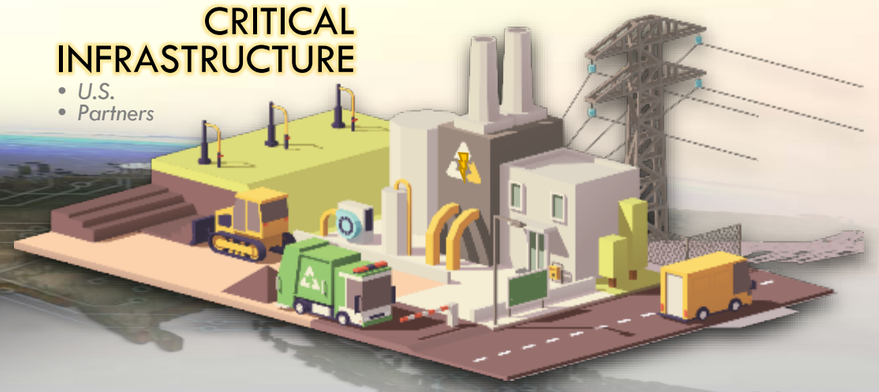
Insider Threat

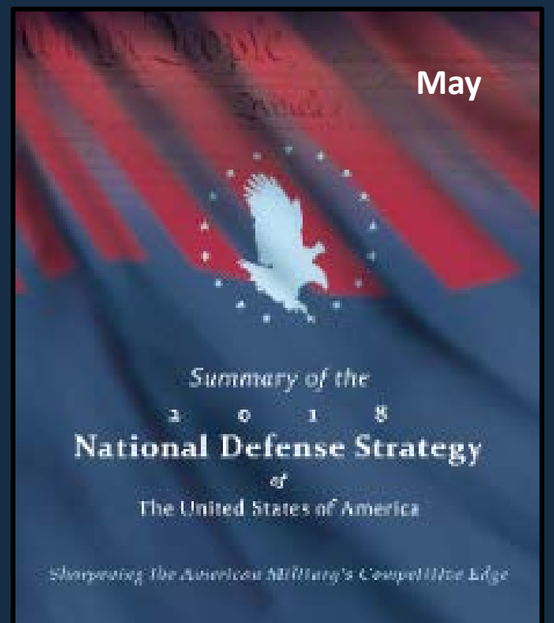
Cybersecurity Culture

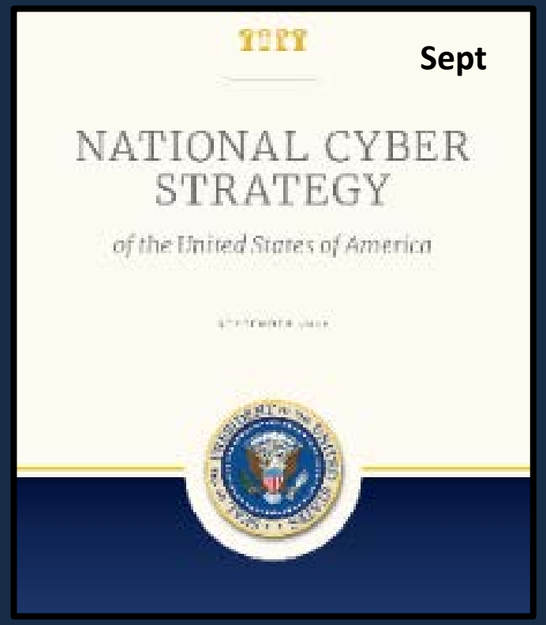
IT PRODUCT/ SUPPLY CHAIN RISK MGMT

CRITICAL INFRASTRUCTURE

- *U.S.*
- *Partners*

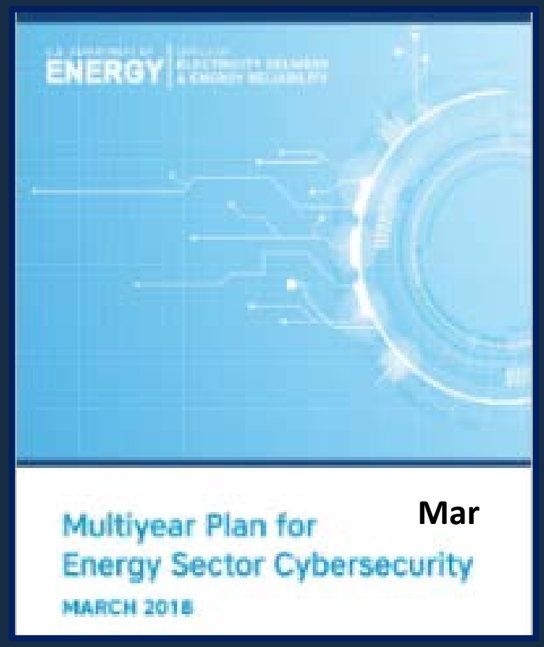



May
Summary of the
2018
National Defense Strategy
of
The United States of America


Sept
NATIONAL CYBER STRATEGY
of the United States of America


Sept
SUMMARY
DEPARTMENT OF DEFENSE
CYBER STRATEGY
2018


IT
OT / CS


ENERGY
Multiyear Plan for Energy Sector Cybersecurity
MARCH 2018
Mar

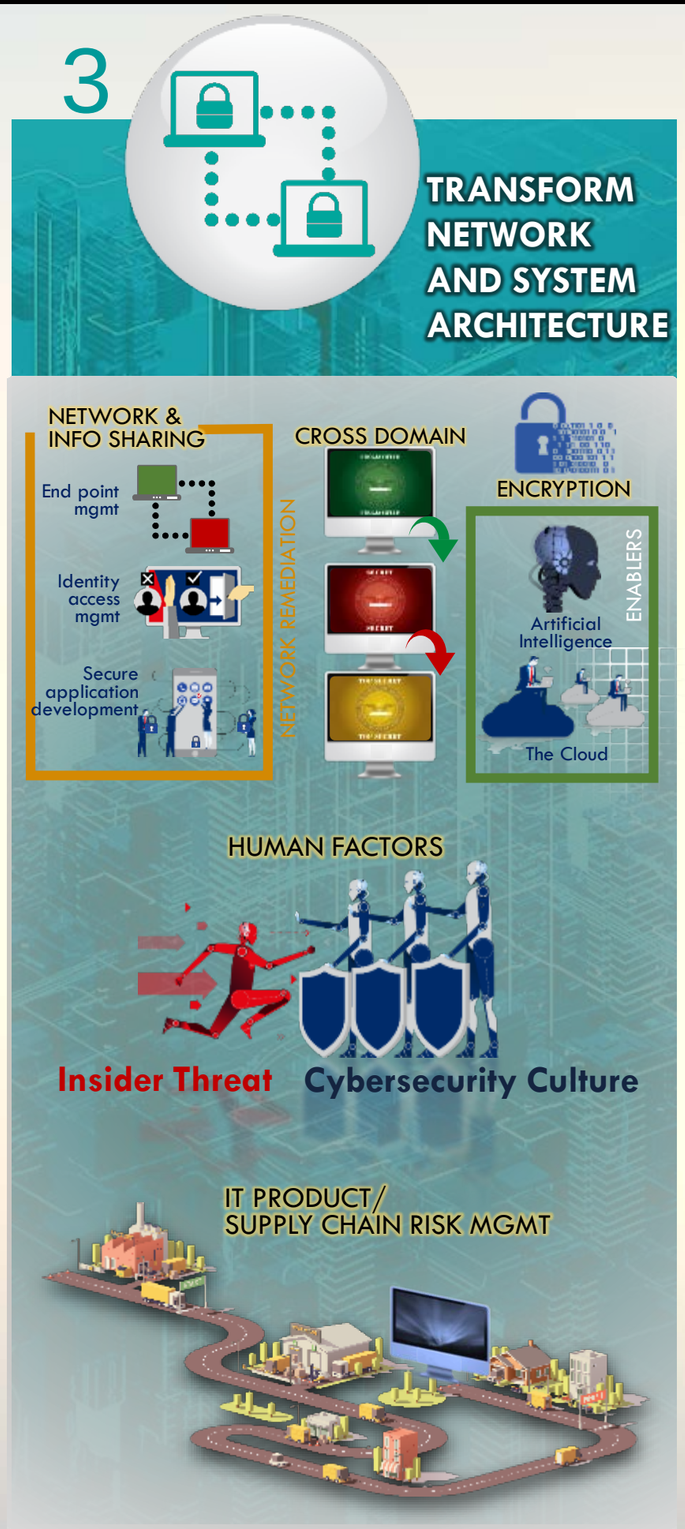

U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY STRATEGY
May 15, 2018
May

DoD Cyber Strategy Lines of Effort

1

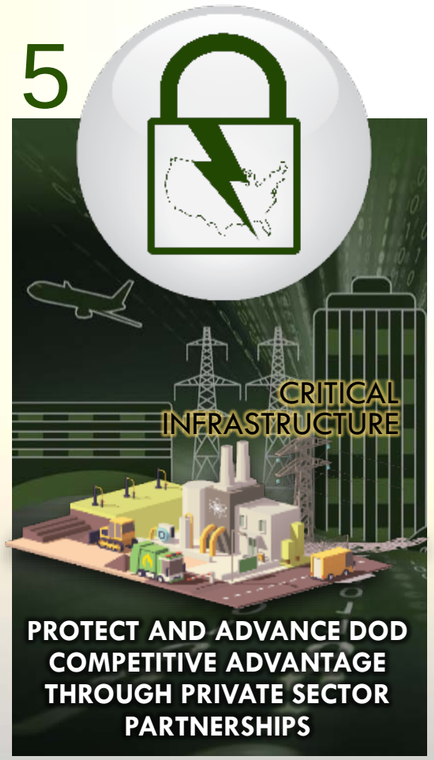
2

3



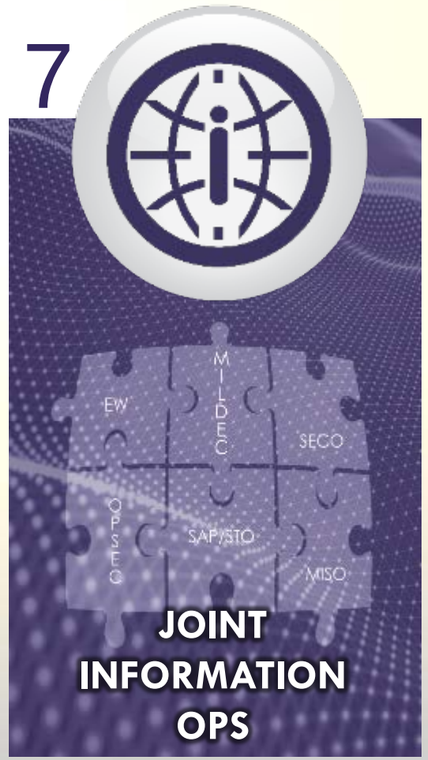
4

5

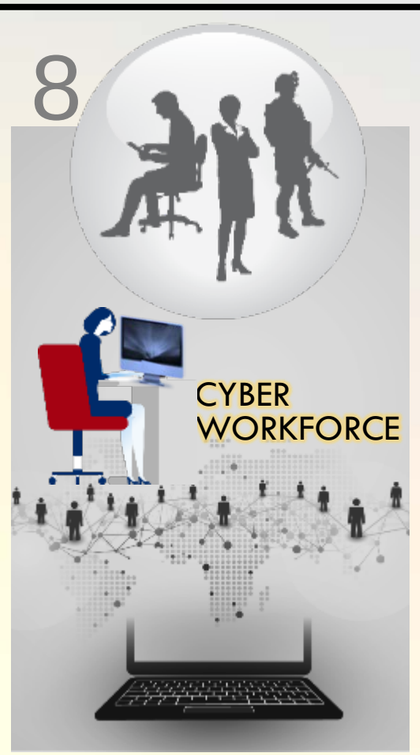


6

7



8

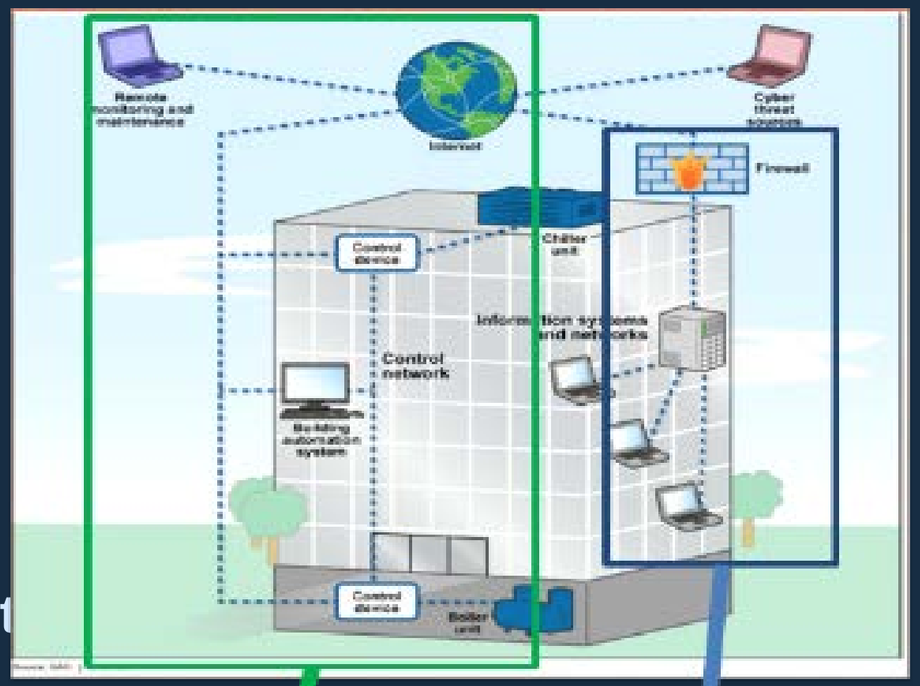


9

Terminology Decisions Needed

PIT, CS, PIT-CS, ICS, FRCS, OT, SCADA, CPS, IoT, IIoT

- ⊘ PIT = Platform Information Technology
- ⊘ ICS = Industrial Control Systems
- ⊘ FRCS = Facility-Related Control Systems
- ⊘ OT = Operational Technology
- ⊘ SCADA = Supervisory Control And Data Acquisit
- ⊘ CPS = Cyber Physical Systems
- ⊘ IoT = Internet of Things
- ⊘ IIoT = Industrial IoT
- ✓ CS = Control Systems
- ~~POT = Platform Operational Technology~~



PIT, CS, ICS, FRCS, OT, SCADA, CPS, IoT, IIoT

Information Systems

Existing Integration Systems

Acuity Brands Roam Advantage Controls ALC Alerton AIE Alerton BACtalk Alerton BCM-WEB American Auto-Matrix Auto Pilot American Auto-Matrix Andover Controls Continuum Asi controls Auto Matrix Sage Automated Logic WebCTRL Automated Logic Barber Coleman Network 8000 Bristol Babcock CAPRON Carrier Carrier Comfort Network Carrier Com-Trol Control Microsystems SCADAPack Cylon Unitron UC32 Daikin Data Aire Dell Vostro Delta Controls ORCA Distech Echelon i.Lon Emerson-Liebert EXHAUSTO Flygt ITT Industries APP 700 General Electric WESDAC General Electric Honeywell Excel 5000 Honeywell WEBs-AX HSQ Technology Invensys I/A Series Invensys Micronet Invensys Network 8000 Johnson Controls Facility Explorer Johnson Controls Metasys Johnson Controls M-Series KMC LANDIS Landis & Staefa Integral MS2000 Landis & Staefa Liebert SiteGate LOYTEC Electronics L-VIS Lynxspring JENEsys Merlin Gerin PowerLogic Microwave Data Systems Mitsubishi Motorola SCADA Systems Odessa Engineering OmniaPRO Orion Controls Paragon EC7000 Series Raco Reliable Controls MACH-ProWebSys Richards-Zeta Robert Shaw DMS RUGID Schneider Electric I/A Series Schneider Electric PowerLogic Siebe Network 8000 Siemens ACCESS Siemens Apogee Siemens Desigo PX Siemens Synco 700 Staefa Staefa/Siemens STULZ Air Technologies TAC I/A Series TAC Network 8000 TAC Xenta TAC Vista Telvent Smart Grid Solution Trane Tracer Trane Tracer Summit Trane Varitrac TREND Trend Control Systems IQ2 Tridium Vykon

Existing Operating Software

Axon CAT SARL Desigo Insight KNX STANDARD ABB Symphony Plus OptimaxRev 4 ABB Symphony Plus 800xA SV 5.1 ABB Symphony Plus Composer 6.0 ABB Symphony Plus S+ Operations 1.1 Alerton BACTalk Envision 2.0 Alerton BACTalk Envision 2.6 Alerton VisualLogic Allen-Bradley RSLogix 500 Allen-Bradley RSLogix 500, RSView32 Automated Logic ExecB 6.0 Automated Logic SuperVision WebCTRL 5.5 Automated Logic WebCTRL WebCTRL 3 Automated Logic WebCTRL WebCTRL 3.0 Automated Logic WebCTRL WebCTRL 5 Automated Logic WebCTRL WebCTRL 5.2 Automated Logic WebCTRL WebCTRL 4.1 SP1 Automated Logic WebCTRL WebCTRL Automated Logic ExecB 4.1 SP1 Automated Logic ExecB drv_lge_4-02-175 Automated Logic ExecB drv_melgr_vanilla_4-02-175 Automated Logic ExecB Automated Logic Supervision 2.6b Automated Logic WebCTRL 4 SP1B Automated Logic WebCTRL 4.1 SP1 Automated Logic WebCTRL 4.1 SP1b Automated Logic WebCTRL SVR 5.5 Calsense Command Center 4.15.11.20 Carrier Comfort Network Comfort Network 3.0 Control Microsystems ClearSCADA 2009 Ed. R2.2 Data flow Systems HyperTAC 2 Data flow Systems HyperTAC HT3 Delta Controls ORCA ORCAview 3.30 Delta Controls ORCA ORCAview 3.40 Delta Controls Orcaview 3.22 Delta Controls Orcaview 3.30 Delta Controls OrcaView 3.3 Delta Controls Orcaview 3.33 Delta Controls Orcaview Delta Controls, TAC ORCA, I/NET ORCAview, Seven Rel 2.15 EFACAC Prism ERI Siemens Insight 3.6 GE, Intellution Proficy, iFIX, FIX Desktop _, _,4.0, _ General Electric Cimplicity Plant Edition 6.1 General Electric Multilin Config Pro 5.03 General Electric Proficy Cimplicity 7.0 General Electric Proficy iFIX 4.0 Honeywell Symmetre Station 3.5 Symmetre 3.5 Honeywell Webstation-AX Niagara Niagara 3.5.40.1 HSQ Miser 6.06 HSQ Miser HSQ, Sun Microsystems Miser, Xview 6.06 Iconics Genesis32 Genesis32 8.3 Iconics Genesis32 Genesis32 9.13 Iconics HMI SCADA Solutions Genesis 32 3.12.005 InduSoft Web Studio Intellution 7 Intellution FIX32 3.5 Intellution FIX32 Intellution iFIX 3.5 Intellution IFIX Intellution iFIX Reporter ITT Flygt AquaView AquaView 1.50 Johnson Controls Metasys 6.0.0.9000 Johnson Controls Metasys GX9100 7.05A Johnson Controls Metasys Metasys 5 Johnson Controls Metasys Metasys 5.1 Johnson Controls Metasys Project Builder 5:1 Johnson Controls Metasys Project Builder 3 Johnson Controls Metasys 5 Johnson Controls Metasys 12.04 Johnson Controls Metasys 2.0.0.70.0 Johnson Controls Metasys 5.2.0.5400 Johnson Controls Metasys Johnson Controls M-Graphics 5.3 Microsoft Explorer N/A N/A N/A N/A Pneu-Logic Pneu-Logic RACO RACO 3.14 Rainbird MAXICOM2 Central Control 4.3 ReLab Software ClearView-SCADA 7.2.8 Reliable Controls MACH ProWebSys RC-Studio 2.0 Robert Shaw Digital Management System Operator Interface 11.0 Rockwell FactoryTalk Service Platform 2.30 Rockwell FactoryTalk View, Rsview Site Editiion, Supervisory 6.0, 6.0 Rockwell Factory Talk 6.0 Rockwell Automation FactoryTalk View Machine Edition 5.1 Rockwell Automation FactoryTalk View Site Edition 4.0 Rockwell Automation FactoryTalk View Site Edition 5.1 Rockwell Automation FactoryTalk View Site Edition Rockwell Automation RSView Supervisory Edition 4.0 Rockwell Automation RSView Supervisory Edition Rockwell Automation RSView32 7.600.00 ScadaTEC SCADASIS 5.8.14.213 Schneider Electric PowerLogic ION Enterprise 5.6 Schneider Electric PowerLogic ION Enterprise Siebe Network 8000 Signal 4.4.1 Siemens S7 300 STEP 7 Siemens Apogee Insight Siemens Desigo Insight Siemens Insight Desigo Insight 2.31 Siemens Insight Desigo Insight 2.35.021 Siemens WinPM.Net 3.2 SP3 SUBNET Solutions SubSTATION Explorer 1.3.0 SUBNET Solutions SubSTATION Explorer 1.5.7 Sun Microsystems Xview 3.2 Symantec Backup Exec 2011? TAC 1/A Series WorkPlace Tech 5.7 TAC I/A Series Workbench TAC I/A Series WorkPlace Tech 5.7.2 TAC 4.1 TAC Signal, XPSI & ZPSIPC Teletrol eBuilding Telvent OaSys DNA 7.4.* Trane Tracer SC Tracer 3.5 Trane Tracer Summit Tracer 11 Trane Tracer Summit Tracer 16 Trane Tracer Summit Tracer 17 Trane Tracer Summit V14 Tracer 14 Trane Tracer Summit V16 Tracer 16 Trane Tracer Summit V17 Tracer 17 Tridium Vykon Niagara 2.301.428 Tridium Vykon Niagara 2.301.430.v1 Tridium Vykon Niagara 2.301.431.v1 Tridium Vykon Niagara 2.301.514 Tridium Vykon Niagara 2.301.514.v1 Tridium Vykon Niagara 2.301.522 Tridium Vykon Niagara 2.301.522.v1 Tridium Vykon Niagara 2.301.522.v2 Tridium Vykon Niagara 2.301.522V1 Tridium Vykon Niagara 2.301.527.v1 Tridium Vykon Niagara 2.301.529 Tridium Vykon Niagara 2.301.532 Tridium Vykon Niagara 2.301.532.v1 Tridium Vykon Niagara 3.3.31 Tridium Vykon Niagara 3.5.34 Tridium Vykon Niagara Workbench 3.6.31 Tridium Vykon Niagara Tridium Vykon Niagara AX 3.3.22.0 Tridium Vykon Niagara AX 3.5.25.0 "Tridium Vykon Niagara AX 3.5.25.0 3.3.22.0" "Tridium Vykon Niagara AX 3.5.25.0 3.4.51.0" Tridium Vykon Niagara AX 3.5.25.1 Tridium Vykon Niagara AX 3.5.34.0 Tridium Vykon Niagara AX 3.5.34.2 Tridium Vykon Niagara AX 3.5.39.0 Tridium Vykon Niagara AX 3.5.40.7 Tridium Vykon Niagara AX 3.5.7.0 Tridium Vykon Niagara AX 3.6.31.0 Tridium Vykon Niagara AX 3.6.31.4 Tridium Vykon Niagara AX 3.6.47 Tridium Vykon Niagara AX 3.6.47.0 Tridium Vykon Niagara AX Tridium Vykon Niagara R2 2.301.522 Tridium Vykon Niagara R2 2.301.522.v1 Tridium Vykon Niagara R2 2.301.529.v1 Tridium Vykon Niagara R2 2.301.532.v1 Tridium Vykon Niagara R2 R2.301.529 Tridium Vykon Niagara R2 Tridium Vykon Niagra 3.5.34.7 Tridium Vykon Workplace Pro 2.301.428 Tridium Vykon Workplace Pro 2.301.514 Tridium Vykon WorkPlace Pro 2.301.522 v2 Tridium Vykon Workplace Pro 2.301.532 Wonderware Intouch WindowViewer 10.1.200 Yokogawa Exaquantum EXAOPC R3.21 Yokogawa Exaquantum Exaquantum Server R2.60 Yokogawa DAQOPC for DARWIN R3.01 2 6.0 ACS Alerton 3.5.34 Alerton Apogee 2.8 BACnet CSIView 11.5.0 build 121 DAQ Works V1.03 Delta-V 7.4 Delta-V DOS 6.2 ERI Excel add -in I/Net 1.02 I/Net 5.1.3-57 I/Net 5.1.4-59 I/Net INET 2000 1.11 build 170 Insight Metasys Power Xpert Software PR970 Prism Protech Siemens 11 SteamEye Symmetre Station 3.5 Tracer Summit 15.0 Versaterm, Crystal Reports VMware WEStation WIN UPM2 Workbench 2.301.522 Workbench 2.310.514

Existing Device Level Controllers

- AAEON Electronics AAON SS1016 ABB ACH550-UH-045A-4 ABB ACH550-UH-04A1-4 ABB ACH550-UH-246A-4 Acuity Brands Roam Gateway ADDER ADDERLink INFINITY ALIF 1000R-US ADDER ADDERLink INFINITY ALIF 1000T-US Advantech Touch Panel Computer TCP-1770H-C2BE Advantech Touch Panel Computer TPC-1780H Advantech Touch Panel Computer TPC-650H AEG BLR-CX 04R AEG Schneider Automation Modicon Micro 612 Alerton VLC-1188 Alerton VLC-444 Alerton VLC-550 Alerton VLC-853 Alerton BACtalk BCM-PWS Alerton BACtalk VAV-SD Alerton BACtalk VLC-1180 Alerton BACtalk VLC-1188 Alerton BACtalk VLC-444 Alerton BACtalk VLC-550 Alerton BACtalk VLC-651R Alerton BACtalk VLC-660R Alerton BACtalk VLC-853 Allen-Bradley Allen-Bradley CompactLogix L23E Allen-Bradley CompactLogix L32E Allen-Bradley ControlLogix 1756-A10 Allen-Bradley ControlLogix 1756-L61 Allen-Bradley ControlLogix OEM Allen-Bradley FlexLogix 1794-L34 Allen-Bradley FlexLogix 5433 Allen-Bradley FlexLogix FLEX I/O Allen-Bradley Integrated Display Computers 6181P Allen-Bradley MicroLogix 1000 1761 Allen-Bradley MicroLogix 1000 1761-L16BWB Allen-Bradley MicroLogix 1100 1763 Allen-Bradley MicroLogix 1100 1763-L16AWA Allen-Bradley MicroLogix 1100 1763-L16BWA Allen-Bradley MicroLogix 1400 Allen-Bradley Micrologix 1400 1766-L32AWAA 8/10.00 Allen-Bradley MicroLogix 1500 1764-24AWA Allen-Bradley MicroLogix 1761-NET-ENI Allen-Bradley PanelView Plus 1000 Allen-Bradley PanelView Plus 2711P-KM420D Allen-Bradley PanelView Plus 600 Allen-Bradley PanelView Plus 700 Allen-Bradley PowerMonitor 3000 Allen-Bradley PowerMonitor 3000 1404-DM A Allen-Bradley PowerMonitor 3000 1404-M405A-ENT B Allen-Bradley SLC 500 DH-485 Allen-Bradley SLC 500 SLC 5/00 Allen-Bradley SLC 500 SLC 5/02 Allen-Bradley SLC 500 SLC 5/03 Allen-Bradley SLC 500 SLC 5/04 Allen-Bradley SLC 500 SLC 5/05 Allen-Bradley VersaView 1500P Andover Controls Continuum Infinet II i2810 Andover Controls Infinity SCX 920 APC AP7960 APC PNET 1 APC Back-UPS BE350R APC Back-UPS BE750G APC Back-UPS BX900R APC Back-UPS ES550 APC Back-UPS Pro 1000 APC Back-UPS RS800 APC Back-UPS XS1500 APC Smart-UPS 1000XL APC Smart-UPS 2200 APC Smart-UPS 2200XL APC Smart-UPS 750 APC Smart-UPS AP5719 APC Smart-UPS SMT3000RM2U APC Smart-UPS SU2200NET APC Smart-UPS SU220RMXL APC Smart-UPS SU3000RMXL APC Smart-UPS SU3000XLM APC Smart-UPS SUA1000RM1U APC Smart-UPS SUA1500 APC Symettra APC Symmetra AP9617 / Symmetra 40K Arena EX III Arista ARP-2217AP Armstrong SteamEye Gateway 3000M Autoflame DTI MK6DTI Automated Logic LGR1000 Automated Logic LGR25 Automated Logic M line M0100 Automated Logic M line M220nx Automated Logic M line M4106 Automated Logic M line M8102 Automated Logic M line M8102nx Automated Logic M line Mcpu Automated Logic ME812u line ME812u Automated Logic S line S6104 Automated Logic U line UNI/32 AutomationDirect DL06 AutomationDirect DL205 AutomationDirect EA7-T10C AutomationDirect EA-T10C AutomationDirect C-More EA7-T6CL AVG EZ-T10C-F AVG EZ-T15C-FSU Axiomtek DIN-rail Embedded System rBOX201-4COM-FL Axis 214 PTZ Axis 2400PTZ Axis 241Q Axis P5512 B&B Electronics MES1B Badger Meter Disc Series 120 Badger Meter Disc Series 170 Badger Meter Disc Series 35 Badger Meter Disc Series 70 Badger Meter M Series 4000 Badger Meter Turbo Series 2000 Badger Meter Turbo Series 450 Barber Coleman Network 8000 MZ2A Basler Electric BE1-25 Basler Electric BE1-700V Basler Electric BE1-CDS220 Basler Electric BE1-GPS100 E3N2R0U Bay Controls BayNet Belkin F6C1100-AVR Belkin F6C750-AVR Bitronics PowerPlex MTWIN3 Black Box ME838A-R2 Black Box ME838A-R3 BOCA Bristol Babcock DPC 3335 Brother HL-2270DW Brother HL-4040CDN Brother HLYOC Buffalo TS-H0.0TGL\RG Buffalo TeraStation Pro TS-H03TGL-R5 CalAmp VIPER SC Campbell Scientific CR1000 Carel pCO3 Carrier 30RRB06052_00__3 Carrier 30XAB50062-03X93 Carrier Comfort Network Comfort Controller 6400 Cohen OEM Computrol 32X Control Microsystems 5000 Series 5302 Control Microsystems SCADAPack 100 Control Microsystems SCADAPack 334 Cooper Power Systems CL-6A Cooper Power Systems CL-6A WA366B67G6AR Cooper Power Systems CL-6A WE383F44K6XR CyberPower 1500ADR CyberPower CPS1500AVR Cylon Unitron UC32 Daikin McQuay MicroTech II WMC Danfoss OEM Danfoss BACLink VLT DEC LA400-A2 Dell 3000CN Dell 71PXP Dell UPS1000W Dell Color Laser Printer 1320C Dell Laser Printer 1110 Dell Laser Printer 2330dn Dell Laser Printer 3100CN Dell PowerValut MD3000i Dell PowerValut TL2000 Delta Controls ORCA DSC-1212E Delta Controls ORCA DSC-1616E Delta Controls ORCA DSC-633E Deltak OEM Digi AccelePort C/X (1P) 50000598-01 Digital Loggers Web Power Switch III Dolch ORCA-19 Dolch ORCA-19PM DROBO 902-00001-001 Eason Technology 950 Eaton RO LIC-100 HMI Eaton Power Xpert PX4000 Eaton Powerware 3105 Eaton Powerware 5125 Eaton Powerware 9125 Eaton Powerware FE2.1KVA Eaton Powerware PW9130L1500T-XL Electro Industries Nexus 1262 Electro Industries Nexus 1270-S-SWB2-20-60-4IPO-SE Electro Industries Nexus 1272 Electro Industries Shark 100S elo Touch Solutions Touch systems Elo Touch Solutions Touchmonitor ET1739L Elo TouchSystems Elster American Meter 3.5M Elster American Meter AL-425 Elster American Meter AL-800 Elster American Meter GT-3 Elster American Meter RPM Series 1.5M Elster American Meter RPM Series 2M Elster American Meter RPM Series 3.5M EMC CLARiiON CX4-120 Emerson M-Series MD Plus Encorp KWS GDU Encorp KWS2222501 Encorp UPC GDU Endress+Hausser Promass 80 Endress+Hausser Prowirl 72W EPSON FX 2190 Fireye Nexus NX6100 Flygt ITT Industries APP 700 APP700F Fuji HDC 500 Fuji Micrex-F F120S F120S Fuji Micrex-SX SPH3000MM Gamewell 1033502501VD General Electric 16SB1BB339SSS2V General Electric 16SB1CB201SDM2Y General Electric 510-0183-01A General Electric 526-2006 General Electric IC695ETM001 General Electric Fanuc 90-30 IC693CPU311 General Electric Fanuc 90-30 IC693CPU311-AD General Electric Fanuc 90-30 IC693CPU311-AE General Electric Fanuc 90-30 IC693CPU311-BE General Electric Fanuc 90-30 IC693CPU311N General Electric Fanuc 90-30 IC693CPU311T General Electric Fanuc 90-30 IC693CPU311W General Electric Fanuc 90-30 IC693CPU311-XX General Electric Fanuc 90-30 IC693CPU311Y General Electric Fanuc 90-30 IC693CPU350 General Electric Fanuc 90-30 IC693CPU352 General Electric Fanuc 90-30 IC693CPU360 General Electric Fanuc 90-30 IC693CPU363 General Electric Multilin 469 General Electric Multilin 750P5G5S5HIA20R General Electric Multilin SR489-P5-HI-A20 General Electric Multilin SR74555HI485 General Electric PACSystems RX3i General Electric PQMII PQMII General Electric RRTD RRTD General Electric Rx3i PacSystem IC694MDL240 General Electric Rx3i PacSystem IC694MDL940 General Electric Rx3i PacSystem IC695ALG112 General Electric Smart Meter kV2c General Electric SR 745 General Electric SR 750 General Electric Versamax IC200CPUE05 Genicom 3850 Hach SC100 Hadax Series 6000 Heliodyne Delta-T Pro Honeywell HC900 Honeywell XL50-MMI Honeywell Excel 5000 Q7055A BNA- Honeywell Excel 5000 Q7750A-2003 Honeywell Excel 5000 XC5010 Honeywell Excel 5000 XCL5010 Honeywell Excel 5000 XL100 Honeywell Excel 5000 XL100C Honeywell Excel 5000 XL20 Honeywell Excel 5000 XL50 Honeywell Excel 5000 XL5010 Honeywell Excel 5000 XL5010C Honeywell Excel 5000 XL50-MMI Honeywell Excel 5000 XL80 Honeywell Excel 5000 XLC50 Honeywell Excel 5000 XLC5010 Honeywell Excel 5000 XLC50-MMI Honeywell Excel 5000 XLC8010 Honeywell Excel 5000 XLC8010A HP HP 700/43 HP 8100 ELITE HP Color LaserJet 4500 HP Color LaserJet CP2025 HP Deskjet 6122 HP InkJet BC354A HP Jetdirect 170x J3258B HP LaserJet HP LaserJet 02461A HP LaserJet 4 HP LaserJet 4600n HP LaserJet 4MV HP LaserJet 5 C3916A HP LaserJet 5200tn HP LaserJet C3980A HP LaserJet CB94A HP LaserJet CP2025 HP LaserJet CP2025DN HP LaserJet CP5225DN HP LaserJet P1102W HP LaserJet P2015 HP LaserJet P4014dn HP OfficeJet 7000 E809a HP Officejet CM755A/8500A HP StorageWorks Tape Array 5300 HSQ Technology HSQ Technology 22501 HSQ Technology 86004862 HSQ Technology 8600-4862 HSQ Technology 8600-6135L HSQ Technology 8602 HSQ Technology 8602-080 HSQ Technology 8602-080A Rev E HSQ Technology 8602-RTU-080-A Rev E HSQ Technology HSQ9588T HSQ Technology V86VR-R030 iEi Technology AFOLUX LX AFL-12A Infinias Intelli-M eIDC Invensys Invensys I/A Series FCM 10E Invensys I/A Series UNC-520-2 ITRON IX100X Johnson Controls Johnson Controls Facility Explorer FX-PCG2611 Johnson Controls M Series MS-N30 Supervisory Controller Kiltech Embedded Field Controllers SX-CPU/RS-485 190715 Koyo DL205 Koyo DL206 Koyo DL207 Koyo DL250 CPU Landis & Staefa Integral MS2000 NRK16-NICO Landis & Staefa Integral RSA NRK16/A Lantronix Lantronix Universal Device Server UDS100 Lexmark Optra E312L LG V-NET PQNFB17B0 Liebert StieLink 12 Liebert StieLink 4 LOYTEC Electronics LINX LINX-101 LOYTEC Electronics L-VIS LVIS-3E100 LOYTEC Electronics L-VIS ME215 Maple Systems OIT3175 Maple Systems OIT3250-B00 Maple Systems PC217B Mcquay H62PY McQuay Maverick I OM 1077 MCS MCS-R010 MechoShade Systems SunDialer I-Con Meidensha ADC5000 Meidensha T01E-E01A Meidensha T01E-E01A-A Meidensha Uniseque RC500 MGE UPS SYS UPS 1500 MGE UPS SYS UPS 800 Mitsubishi Mitsubishi AG-150A Mitsubishi MP-22-AF Mitsubishi MP-22-AR Mitsubishi MP-22-CB Mitsubishi CITY MULTI BAC-HD150 Mitsubishi CITY MULTI GB-50ADA Mitsubishi MELSEC Q63P Mitsubishi Q Series FX2N Modicon Micro Modicon Momentum 170ADM39030 Modicon Quantum Automation Series 140CPU113 MODICON TSX Quantum Modicon TSX Series TSX3705028 Modicon TSX TSX3705028 Motion Control Engineering Motion Control Engineering 24-10-0012 Motorola MOSCAD-L Motorola SCADA Systems ACE3600 Moxa MGate IMC-101-M-SC Nalco Switch 2226 3D Trasar NETGEAR ReadyNAS 3200 NETGEAR ReadyNAS Pro NOVAR NL INC B541200039 NovaTech Orion5r Obvius Holdings AcquiSuite A8812 Odessa Engineering DiaLog Plug Okidata MicroLine 321 Turbo Okidata MICROLINE ML420 OMNTEC OEL8000II OEL8000IIP Opto 22 Opto Brian Panasonic BB-HCM531 Panasonic GN 15 Panasonic i-Pro WV-NP244 Panasonic i-Pro WV-NS202A Panasonic i-Pro WV-NW964 Patton Copper Link 2156 Perle IOLAN SCS PML ION7350 PML PowerLogic ION7300 PML PowerLogic ION7330 PML PowerLogic ION7350 PML PowerLogic ION7500 PML PowerLogic ION7550 PML PowerLogic ION7600 PML PowerLogic ION7650 PML PowerLogic ION7700 PML PowerLogic ION8600 Pneu-Logic 10A22646 Pneu-Logic PL4000 DCM Powerlynx OEM Preferred Instruments PCC-III Preferred Instruments PCC-III-0000 Preferred Instruments PCC-III-F000 Preferred Instruments PCC-III-FZ00 Pro-Face GP577R-TC11-OY ProSoft MVI46-MNET Qualitrol ITM 509 ITM RACO VERBATIM DFP RACO VERBATIM SFP Raritan CompuSwitch CS4R Raritan Dominion KX II 216 Raritan Dominion KX II DKX2-216 Raritan Dominion KX II DKX2-432 Red Lion G308 Red Lion G310C Ricoh Aficio MP C2050 RUGID RUG6D RUGID RUG7D RUGID RUG9 RUGID RUG9B RUGID RUG9D Sanyo Denki SANUPS A11H Schneider Electric 170INT11000 Schneider Electric 171CCS76000 Schneider Electric HMIPSCIDE03 Schneider Electric Modicon M340 Schneider Electric I/A Series MNB-1000 Schneider Electric Magelis XBT GT 2330 Schneider Electric Momentum Processor 171CCC96020 Schneider Electric Momentum Processor 171CCS78000 Schneider Electric Powerlogic CM2000 Schneider Electric Powerlogic CM3000 Schneider Electric Powerlogic CM4000 Schneider Electric Powerlogic ECC Schneider Electric Powerlogic EGX 100 Schneider Electric Powerlogic EGX 200 Schneider Electric Powerlogic EGX 400 Schneider Electric Powerlogic enercept Meter Schneider Electric Powerlogic Energy Meter Schneider Electric PowerLogic ION7330 Schneider Electric PowerLogic ION7350 Schneider Electric PowerLogic ION7500 Schneider Electric PowerLogic ION7600 Schneider Electric PowerLogic ION7650 Schneider Electric PowerLogic ION8300 Schneider Electric PowerLogic PM710 Schneider Electric PowerLogic PM850 Schneider Electric Powerlogic Power Meter Schneider Electric TSX Momentum Schneider Electric TSX Momentum 171CCC9803 Schneider Electric TSX Quantum 170-ENT-110-00 Schneider Electric Xenta 280 282 Schneider Electric Xenta 300 301 Schweitzer Engineering Laboratories SEL-2020 Schweitzer Engineering Laboratories SEL-2032 Schweitzer Engineering Laboratories SEL-2407 Schweitzer Engineering Laboratories SEL-2411 Schweitzer Engineering Laboratories SEL-2440 Schweitzer Engineering Laboratories SEL-3332 Schweitzer Engineering Laboratories SEL-3530 [illegible] Laboratories SEL-751A Schweitzer Engineering [illegible] Series 200 MEC Siemens Apogee 545-7 [illegible] ower MEC 40 System 600 Siemens Apogee Power Mec Series 200 Siemens Apogee Power Mec System 600 Siemens Apogee PXC100 Siemens Apogee PXC24 Siemens Desigo PX PXC36 Siemens Desigo PX PXC52 Siemens Desigo RCX PXR11 Siemens Desigo RCX PXR12 Siemens HydroRanger 200 7ML50342AA01 Siemens SIMATIC S7-1200 Silex SX-3000GB Solar OEM STULZ Air Technologies Fieldserver DCC828 Symmetricom bc635PCI Symmetricom TrueTime 820-202 Symmetricom TrueTime XL-DC TAC Xenta 302/N/P Teletrol eBuilding Concentrator Telvent Smart Grid Solution SAGE 2300 Telvent Smart Grid Solution SAGE 2400 Terminator T1H-EBC100 Terminator T1H-EBC101 Toshiba OIS-DS52 Total Control Products QuickPanel Trane EMTF000AAC02100 Trane OEM Trane TNS1 Trane UC800 Trane Tracer CH530 Trane Tracer EX2 Trane Tracer MP503 Trane Tracer MP580/581 Trane Tracer MP581 Trane Tracer SC Trane Tracer Summit BCU Transformative Wave Technologies eIQ nSITE 600 Trend Control Systems IQ250 Trend Control Systems NXNI Trend Control Systems XCITE Trend Control Systems IQ2 IQ204 Trend Control Systems IQ21x IQ210 Trend Control Systems IQ21x IQ233 Trend Control Systems IQ21x IQL-SDK Trend Control Systems IQ22x IQ220 Trend Control Systems IQ24X IQ241 Trend Control Systems IQ25X IQ250 Trend Control Systems IQ25X IQ251 Trend Control Systems IQ3s EINC Tridium JACE-403 Trijay Triplite AVR900U USRobotics Uticor 100G-PL08S2R0 Viconics VT7600 WAGO 750-841 Walchem WMT8130-2LNNN Westinghouse WEStation Woodward 505 9907-163 Woodward LinkNet 9905-966 Woodward LinkNet 9905-970 Woodward LinkNet 9905-971 Yokogawa AIP578 Yokogawa AIP578 Style S1 Yokogawa CP40110-S Yokogawa CP703 Yokogawa DA100-11-1M Yokogawa DA100-22-1M Yokogawa DC100-21-11-1M

Difference Between DoD & Commercial Products = None!

DoD CIO Memo Dec'18: (U) RESPONSIBILITIES OF DOD COMPONENTS TO IMPLEMENT CYBERSECURITY FOR ALL DOD CONTROL SYSTEM TYPES

a. (U) Ensure cybersecurity implementation and risk management of control systems, for all DoD systems, adheres to the requirements of the DoD cybersecurity program and mission assurance program, and aligns to the DoD Cyber Strategy and Cyber Posture Review.

b. (U) Designate an office of primary responsibility (OPR) to represent DoD Component on policy and procedural matters regarding cybersecurity for control systems. Regardless of OPR designation, DoD Component CIOs are responsible for compliance with Dept cybersecurity standards in DoD IT and NSS, to include control systems, per Title 10 § 2223.

c. (U) Assign DoD Component organization(s) or program(s) to identify, assess, manage risk, monitor and report for all DoD Component control systems commensurate with supported missions and the value of potentially affected information or assets per DoDI 8500.01.

(e) (U) Ensure cybersecurity requirements for control systems are addressed and visible to DoD Component CIOs in all portfolios, life-cycle management processes, and investment programs.

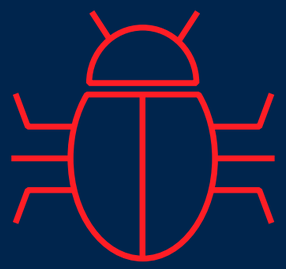
(t) (U) Establish and/or employ blue and red team tools, capabilities, and test environments, as appropriate, to proactively identify, reduce, and mitigate cybersecurity vulnerabilities

(i) (U) Establish and execute a control systems cyber incident handling process in accordance with CJCS Manual 6510.01 B, "Cyber Incident Handling Program."

(j) (U) Identify or establish and maintain cybersecurity education and training requirements for DoD personnel responsible for operating, maintaining, and monitoring control systems and control systems environments.

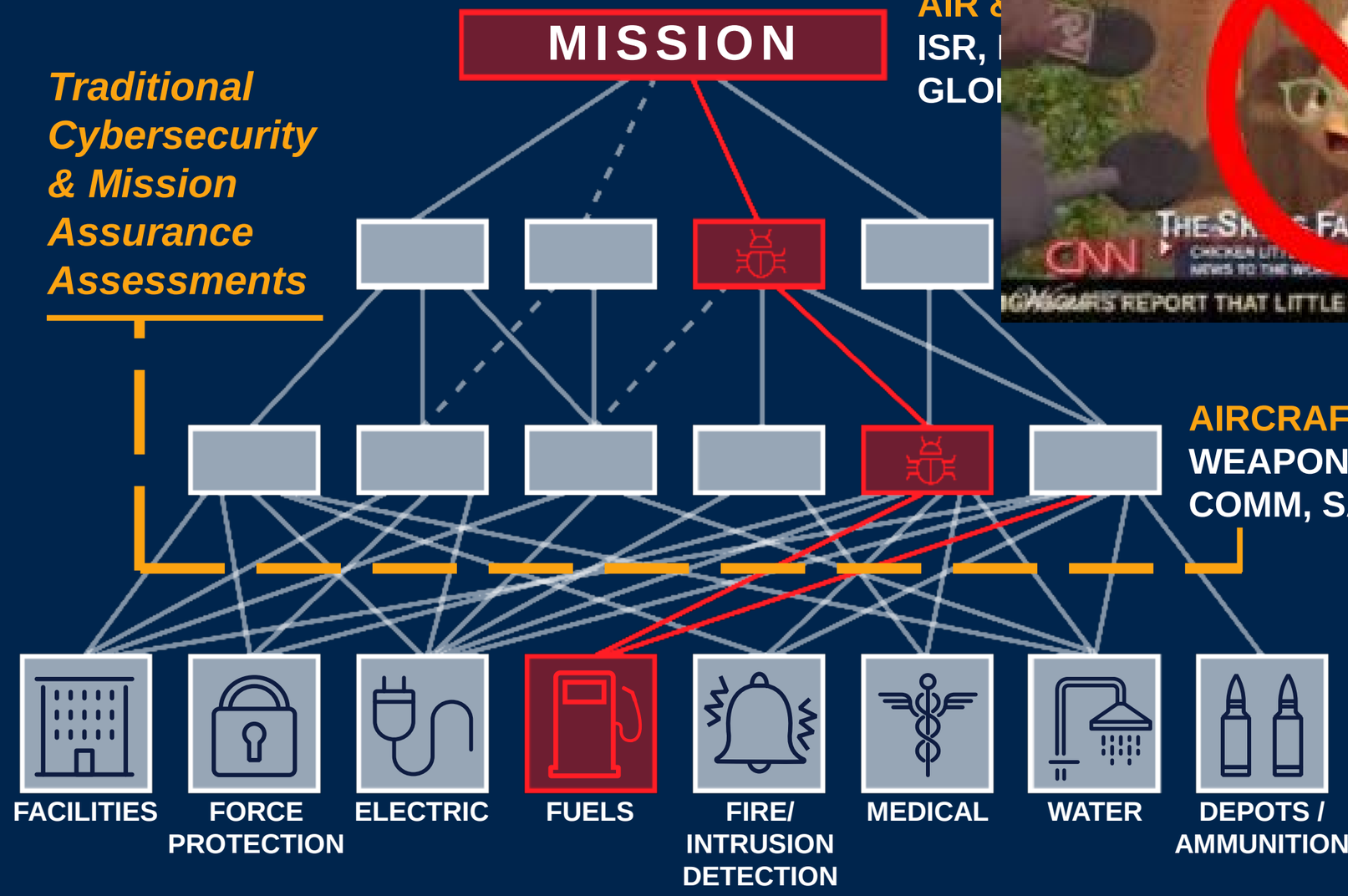
INFRASTRUCTURE VULNERABILITIES DISRUPT MISSIONS

NOTIONAL MISSION THREAD CRITICAL PATH



An adversary could disrupt, degrade, or deny a mission by targeting the foundational assets that underpin the system of systems

Traditional Cybersecurity & Mission Assurance Assessments



Who to Best Defend Control Systems: IT or OT SMEs?

Exec Order on America's Cybersecurity Workforce (May'19): "Cyber-Physical Systems (CPS) for which safety & reliability depend on secure control systems…"

- **Survey to identify & evaluate skill & training gaps in Federal and non-Federal cybersecurity personnel**
  - Critical Infrastructure Sectors
  - Defense Critical Infrastructure
  - DoD Platform Information Technologies (PIT)
  - Collaboratively develop cyber career pathways & competency models

Specific questions to identify:
-Existing skill gaps in CPS workforce
-Underlying cause of skill gaps
-Recommendations to address gaps

Cyber-physical Workforce Survey				Federal, Non-Federal, or Both?:		
24-Jun-19				Sector:		
				Organization/Service/Agency:		
INSTRUCTIONS:				POC Name:		
1. Complete your organizational information starting in cell E1.				POC Phone Number:		
2. Complete survey questions 1-7 in columns E-K for each of the Competency Areas.				POC Email:		
3. Provide additional comments in column L.						
4. If the gap applies, but you are unsure of the answer to the survey questions, please indicate with "?"						
The goal is to derive as much information as possible with this survey - Thank you for your thoughtful support!						
				Survey Question 1	*Survey Question 2*	*Survey Question 3*
Competency and Gap References (based on FBPTA 2018 Update and JHU APL Report for CS Skills)				Does this competency gap exist for CPS in your footprint? (1=Not at All; 2=Somewhat; 3=Moderately; 4=Very Much; 5=Completely)	List additional competency gaps related to this competency associated with CPS in your footprint.	Is the competency gap due to an isssue other than a training gap? If so, describe issue (e.g., personnel shortfall due to hiring difficulties, not enough allowed positions).
Competency Area	Control System Competency	Competency Gap	Training Opportunities			
	Demonstrate familiarity with cyber-physical systems, subsystems, sensors and other components.	Maintain configuration management of CS	ICS-CERT: Intro to Control Systems Cybersecurity NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab			
		Maintain awareness of vulnerabilities to older systems (due to age)				
		Ensure workforce training and procedures for operation of critical equipment				
	Demonstrate familiarity with cybersecurity assessment of CPS.	Maintain network awareness	ICS - CERT: Intermediate Cybersecurity for Industrial Controls Systems, NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, Network Penetration Testing and Computer Networks CS 420 Data Communications ICS-CERT: ICS Cybersecurity Scada hacker: General ICS and Cybersecurity Training NPS: CS Lab, CISR Lab, CS4558 Network Traffic			
		Provide institutional knowledge of system purpose and architecture				
		Provide for identification of new vulnerabilities				

More Situational Awareness of ICS MOSAICS

CS/OT Protection

ICS Operator

Cyber Defender

Control Systems / Operational Technology

Joint Warfighter Operations

Improved Situational Awareness and Speed to Decision

Detect → Analyze → Visualize → Decide → Mitigate → Recover

Smart Integration of Autonomy

Higher Mission Assurance

Water

Electric Grid

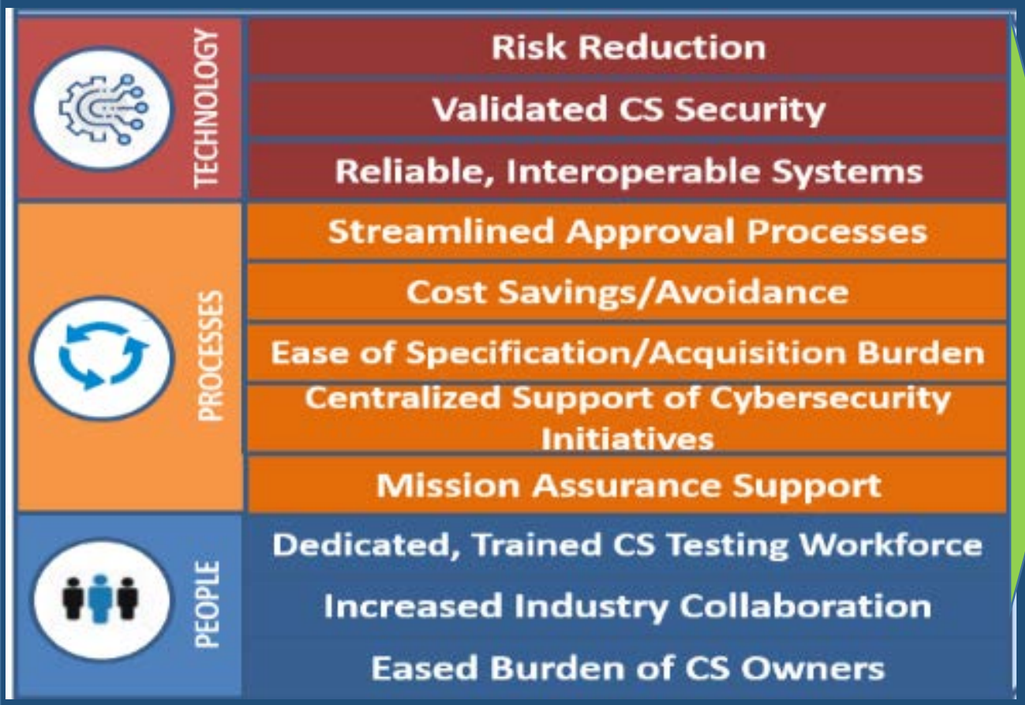
Fuel

Building /Plant

Protect Critical Infrastructure CS / OT from Non-Kinetic Attacks

Control System Tested Product List (CS TPL)

https://www.cs-tpl.com/



Secure DoD Control Systems

CS Acquisition Confidence

Cost Savings / Avoidance

Support of Federal, DoD Initiatives

- Provides list of vetted/tested/approved CS products
- Testing documentation may be reused (Reciprocity and Reuse)
- Reduces Assessor burdens with standard, repeated process
- Fulfills 3rd-Party assessment rqmt
- Facilitates CS acquisition
- Streamlines Cyber testing and RMF authorization processes
- Removes redundancy of multi-site evaluation of same system

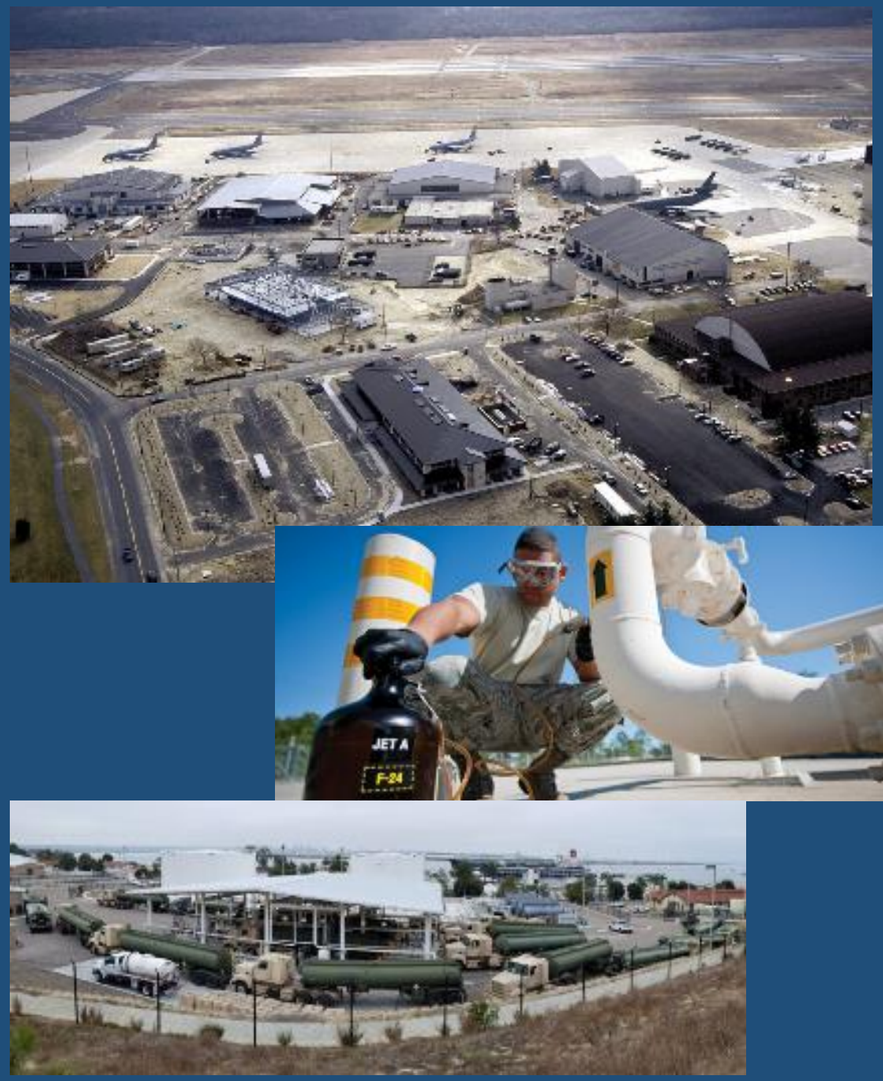
Capabilities Assessment = assist the system designer in determining components which will provide the necessary functionality and security posture in their system IAW of Unified Facilities Criteria 4-010-06 and Unified Facilities Guide Specifications 25-05-11.

Compliance Assessment = assess via Risk Management Framework (RMF) and Control Correlation Identifiers (CCIs) using National Institute of Standards and Technology (NIST) 800-53, 800-82 controls & generate applicable documentation for security assessments and designs.

Study: Understanding Potential Effects & Consequence of Cyber Vulnerabilities on Installation FRCS

Description

- Events have not yet had a significant impact
- Demo may drive cultural & behavioral changes
- Develop ***a plan for a pilot demonstration***
- Provide underpinnings for the design, planning, execution, and assessment of a major, likely multi-year, demonstration leveraging multiple agencies, laboratories, FFRDCs, etc.
- Leverage previous exercise and wargame execution deliverables
- **Effort began Sept'19; complete plan NLT Jun'20**



Cyber Risk to the Department's Installation Infrastructure is Unknown; Focused Cyber Assessments and Mitigations Needed

CYBER RISK MANAGEMENT FOR

UTILITY SERVICE PROVIDERS

Assistant Secretary of Defense for Sustainment (ASD(S)) Supplemental Guidance for the Utilities Privatization Program Memorandum **Feb 7, 2019** requires:

1) “All data required to provide privatized utility services” be handled as Covered Defense Information/Controlled Unclassified Data – new, renewing, and existing utility service contracts

DFARS 252.204-7012
Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.227-7013
Rights in Technical Data - Non-commercial Items

2) Cyber Risk Management Plan (CRMP) for systems owned and operated by Utility Service Provider that process and store CDI/CUI

CRMPs IAW NIST SP 800-171 showing compliance with DFARS

Cyber Risk Management Plan Process for Utility Service Providers - DRAFT

Acquisition and Sustainment

DFARS 252.204-7012
Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.227-7013
Rights in Technical Data - Non-commercial Items

CRMPs IAW NIST SP 800-171 showing compliance with DFARS

Privately Owned?

Yes

No

3rd Party System

JMAA Benchmarks

DoD Mission Assurance Benchmarks IAW DTRA Assessment Guidelines

Cybersecurity Maturity Model Certification (CMMC)*

*** To be issued in 2020**

CRMP
For Corporate IT business systems that host or transmit Controlled Unclassified Information (CUI)

RMF Process

CRMP

- Event/Incident Communications Plan*
- Security Assessment Plan
- Event/Incident Response Plan
- System Security Plan
- Security Audit Plan
- Plan of Actions & Milestones*
- Information Systems Contingency & CONOPS Plan

* To be produced for joint action items with the Services

ESTCP Website

NIST 800-171

CSET Tool

OSD EP

CDRL / Attestation Letter / Data Accession List

Facility Related Control Systems (FRCS) POCs

Army	Navy / USMC	Air Force	DLA
Laura Vaglia	Vish Aswani / Nick Spurling	Jason Burnside	Linus Baker

UP Program Office

Army	Navy / USMC	Air Force
Curt Wexel; Kelvin Herring	Johnathan Currie	Shawn Rose
Office of Deputy Chief of Staff, G-9		AFCEC

System Owners

Contracting Officer (KO)

DLA
Martha Gray; Laurie Carlson
Director, DLA Energy Utility Services; Deputy Director, DLA Energy Utility Services

System Owners

Resources

- **WEBSITE = Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP)**
- **https://serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity**

- **Policies**
- **Contract language**
- **Design & Commissioning**
- **Energy Project / 3rd party**
- **Protecting CUI**


Guidance to Stakeholders for Implementing
Defense Federal Acquisition Regulation Supplement
Clause 252.204-7012
(Safeguarding Unclassified Controlled
Technical Information)

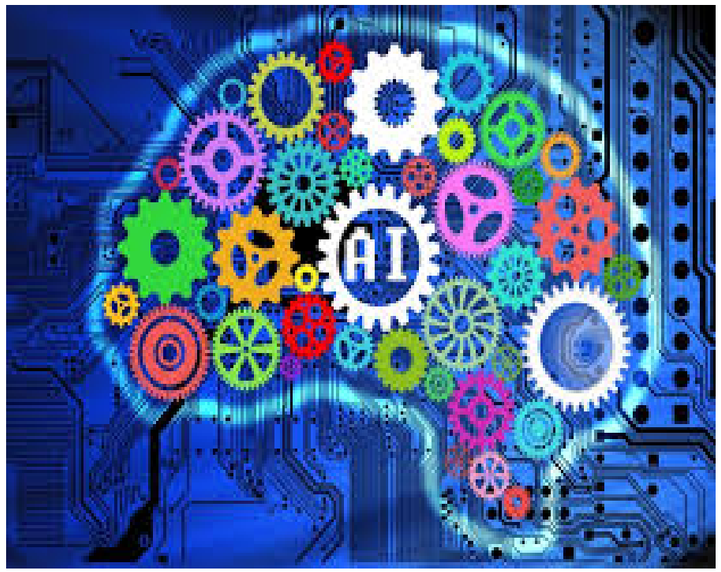
Version 2.0

August 2015

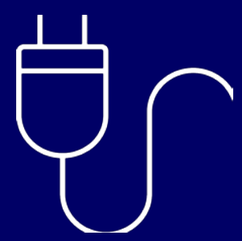
DFARS Technical Information. Technical data or computer software as defined in DFARS Clause 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in the solicitation or contract. **Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.**

Great Place to START! Welcome Suggestions to Improve!

Artificial Intelligence, Machine Learning, Quantum Computing, etc.



All Need:



- **Adversaries are coming and may already be on your network / devices**
- **Know your / vendor systems & devices connectedness**
- **Verify vulnerabilities & risk w/ Implement basic cyber hygiene, best practices**
- **Rehearse! & Report Suspicious System / Device Behavior & Incidents**